



FortiClient EMS - QuickStart Guide

VERSION 1.2.1

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



July 25, 2017

FortiClient EMS 1.2.1 QuickStart Guide

04-121-408698-20170725

TABLE OF CONTENTS

Change Log	4
Introduction	5
Supported installation platforms	5
Required services and ports	5
Deployment options	6
Standalone	6
Integrated with FortiGate	7
Installation	8
Downloading the installation file	8
Installing FortiClient EMS	8
Starting FortiClient EMS and logging in	10
Accessing FortiClient EMS remotely	10
Endpoint Management Setup	11
FortiClient EMS	11
FortiClient EMS integrated with FortiGate	11
Configuring user accounts	12
Adding endpoints	13
Adding endpoints using an Active Directory domain server	13
Connecting manually from FortiClient	14
Creating gateway IP lists	15
Assigning gateway IP lists to endpoints	16
Adding FortiClient installers	16
Configuring profiles	17
Creating profiles to deploy FortiClient	18
Importing FortiGate profiles	19
Preparing Windows endpoints for FortiClient deployment	21
Assigning profiles to endpoints	21
Viewing endpoints	21
Viewing the Endpoints content pane	21
Using the quick status bar	25
Viewing endpoint details	26

Change Log

Date	Change Description
2017-07-06	Initial release
2017-07-25	Clarified when FortiClient EMS can be deployed with Windows workgroups.

Introduction

This guide describes how to install and set up FortiClient Enterprise Management Server (EMS) for the first time. FortiClient EMS is used to deploy and manage FortiClient endpoints.



An informative video introducing you to FortiClient EMS is available in the [Fortinet Video Library](#).

Supported installation platforms

You can install FortiClient EMS on the following platforms:

- Microsoft Windows Server 2012, 2012 R2
- Microsoft Windows Server 2008 R2



For information about minimum system requirements and the latest information about supported platforms, see the *FortiClient EMS Release Notes*, available in the [Fortinet Document Library](#).

Required services and ports

You must ensure that required ports and services are enabled for use by FortiClient EMS and its associated applications on your server. The required ports and services enable FortiClient EMS to communicate with endpoints and servers running associated applications. You do not need to enable ports 8013 and 10443 as these are opened by the FortiClient EMS installation.

Communication	Service	Protocol	Port
FortiClient endpoint/FortiClient Telemetry	File transfers	TCP	8013 (default)
Computer browser service <ul style="list-style-type: none">• Allows FortiClient endpoints to automatically register to EMS. Computer browser service is not needed if an Active Directory is used or endpoint users can manually register FortiClient to EMS.	Enabled		
Samba (SMB) service <ul style="list-style-type: none">• FortiClient EMS uses the SMB service during FortiClient deployment.	Enabled		445

Communication	Service	Protocol	Port
Distributed Computing Environment / Remote Procedure Calls (DCE- RPC) <ul style="list-style-type: none"> The FortiClient EMS server connects to the endpoints using RPC for FortiClient deployment. 	Enabled		135
Active Directory server connection	When used as a default connection		389 (LDAP) or 636 (LDAPS)
FortiClient download	Enabled		10443 (default)
Apache	HTTPS	TCP	443
SQL server			

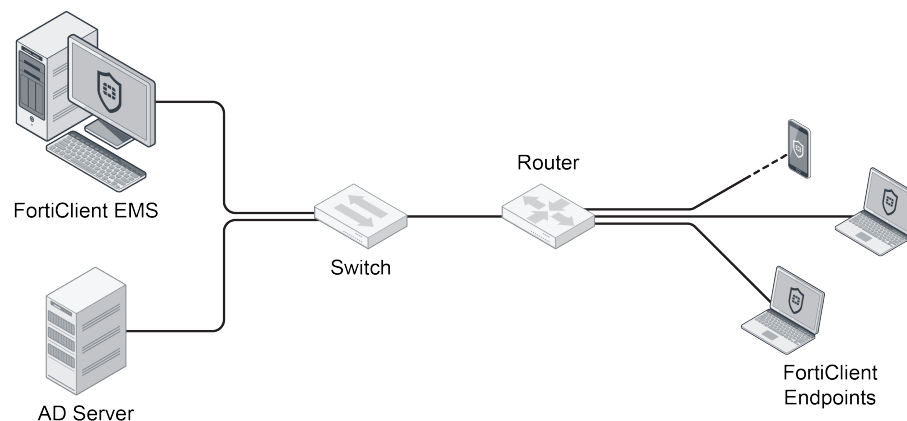


Ensure that the Computer Browser Service is running. On Windows Server 2012 R2, the service is disabled by default. If this service is not active, FortiClient EMS cannot detect computers on the same network, even if they are available.

Deployment options

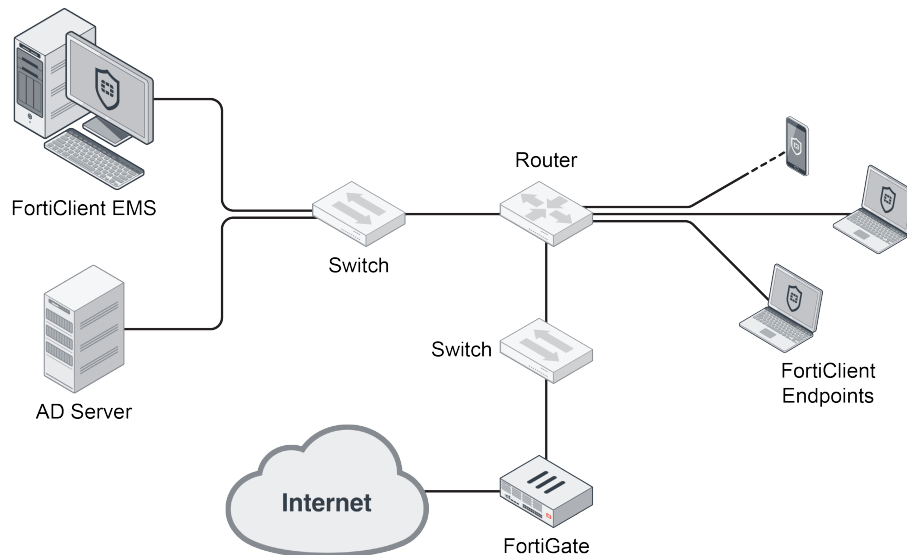
The following deployment options for EMS are supported: standalone or integrated with FortiGate.

Standalone



In standalone mode, a FortiGate device is not required, and network access control (NAC) is not supported. In a standalone mode, EMS deploys FortiClient software on endpoints, and FortiClient endpoints connect FortiClient Telemetry to EMS to receive configuration information from EMS. EMS is used to deploy, configure, and monitor FortiClient endpoints.

Integrated with FortiGate



In integrated mode, a FortiGate device is required, and NAC is supported. In integrated mode, EMS deploys FortiClient software on endpoints, and FortiClient endpoints connect FortiClient Telemetry to FortiGate to receive compliance rules. FortiClient endpoints also connect to EMS to be managed. After FortiClient endpoints are connected, compliance rules are downloaded from FortiGate to the endpoint. EMS might also push a profile of FortiClient configuration information to endpoints. FortiClient endpoints are now managed, and NAC is enforced.

FortiClient uses the compliance rules from FortiGate to communicate whether the endpoint is compliant. If an endpoint fails to meet the compliance rules, the steps required to remain compliant are communicated. For more information, see the *FortiClient Administration Guide*.

Installation

For a complete endpoint solution, FortiClient should be installed on all endpoints, and FortiClient EMS should be installed for central management and provisioning of endpoints.

Following is a summary of how to install and start FortiClient EMS:

1. Download the installation file. See [Downloading the installation file on page 8](#).
2. Install FortiClient EMS. See [Installing FortiClient EMS on page 8](#).
3. Start FortiClient EMS and log in. See [Starting FortiClient EMS and logging in on page 10](#).

For information about upgrading FortiClient EMS, see the FortiClient EMS *Release Notes*.



An instructional video on how to install, log in, and change your administrator password is available in the [Fortinet Video Library](#).

Downloading the installation file

FortiClient EMS is available for download from the following location:

- Fortinet Support website: <https://support.fortinet.com/>

You can also receive the installation file from a sales representative.

The following installation file is available for FortiClient EMS:

- FortiClientEnterpriseManagement_1.2.1.<build>_x64.exe

For more information about obtaining FortiClient EMS, contact your Fortinet reseller.

Installing FortiClient EMS

The FortiClient EMS installation package includes:

- FortiClient EMS
- Microsoft SQL Server 2014 Express Edition
- Apache HTTP server



Local administrator rights and Internet access are required to install FortiClient EMS.

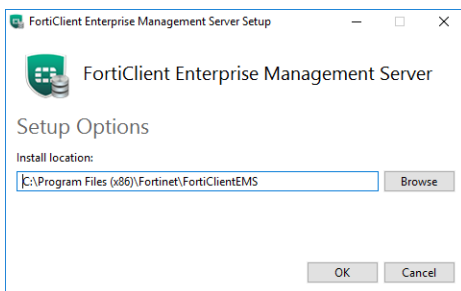
To install FortiClient EMS:

1. If you are logged into the system as an administrator, double-click the downloaded installation file.
If you are not logged in as an administrator, right-click the installation file, and select *Run as administrator* from the pop-up menu.

2. If applicable, select **Yes** in the *User Account Control* window to allow the program to make changes to your system.
3. In the installation window, select **I agree to the license terms and conditions**, if you agree with the license terms and conditions. If you do not agree, you cannot install the software.

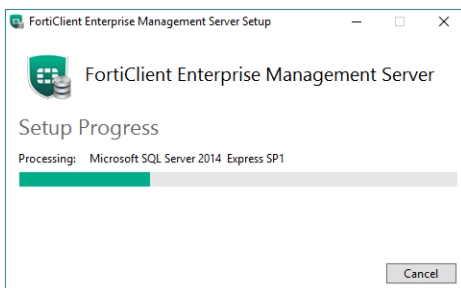


4. (Optional) Click **Options** to specify a custom directory for the FortiClient EMS installation.

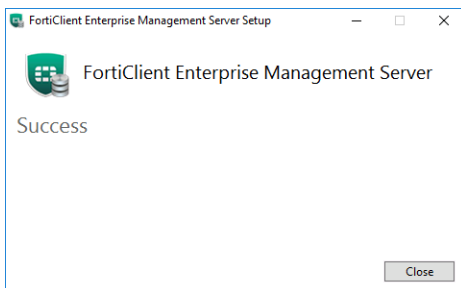


- a. Click **Browse** to locate and select the custom directory.
 - b. Click **OK** to return to the installation wizard.
5. Click **Install**.

The installation may take 30 minutes or longer. It may appear to stop at times, but this is only because certain steps in the installation process take longer than others. Please be patient.



6. When the program has installed correctly, the *Success* window will be displayed. Click **Close** to close the window.



A *FortiClient Enterprise Management Server* icon will be added to the desktop.

Starting FortiClient EMS and logging in

FortiClient EMS runs as a service on Windows computers.

To start FortiClient EMS:

1. Double-click the *FortiClient Enterprise Management Server* icon to start FortiClient EMS.
2. Sign in with username *admin* and no password.
3. Change the username and password by going to *View > User Management > Administration*.
4. Configure FortiClient EMS by going to *View > Settings*.

Accessing FortiClient EMS remotely

You can access FortiClient EMS remotely by using a web browser instead of the GUI.

To enable remote access to FortiClient EMS:

1. Go to *View > Settings*.
2. On the *Server Settings* tab, enable *Remote Administration HTTPS Access*.
3. In the *Custom Host Name* box, type the host name or IP address.
4. Click *Save*.

To remotely access FortiClient EMS:

- To access EMS from the EMS server, visit `https://localhost`
- To access the server remotely, use the server's hostname: `https://<server_name>`

Ensure that you can ping `<server_name>` remotely. This can be achieved by adding it into a DNS entry or by adding it to the Windows hosts file. You may have to modify the Windows firewall rules to allow the connection.

Endpoint Management Setup

This section describes how to set up FortiClient EMS for endpoint management. It provides an overview of using FortiClient EMS as well as an overview of using FortiClient EMS integrated with FortiGate.

When FortiClient EMS is integrated with FortiGate, you can use gateway IP lists to help FortiClient endpoints connect to FortiClient EMS and FortiGate. You can also import FortiClient profiles from FortiGate to FortiClient EMS.

FortiClient EMS

Following is a summary of how to use FortiClient EMS without FortiGate:

1. Configure user accounts. See [Configuring user accounts on page 12](#).
2. Add domains and/or discover local endpoints. See [Adding endpoints on page 13](#)
3. Add a FortiClient installer to EMS. See [Adding FortiClient installers on page 16](#).
4. Create an endpoint profile and select a FortiClient installer. See [Creating profiles to deploy FortiClient on page 18](#).



You can use FortiClient EMS with an Active Directory server to install and upgrade FortiClient on endpoints before and after endpoints connect Telemetry to EMS. You can use FortiClient EMS with workgroups only to upgrade FortiClient on endpoints after they connect Telemetry to EMS and FortiClient registers to FortiClient EMS. When using workgroups, you must separately install FortiClient on endpoints. See the *FortiClient EMS Administration Guide* for details.

5. Prepare Windows endpoints for FortiClient deployment. See [Preparing Windows endpoints for FortiClient deployment on page 21](#).
You must also prepare the Windows AD server for deployment. For details, see the *FortiClient EMS Administration Guide*.
6. Assign a profile to a workgroup or domain, an endpoint group, or an organizational group. See [Assigning profiles to endpoints on page 21](#).
Depending on the configuration of the selected profile, FortiClient will be installed on the endpoints to which the profile is applied.
After FortiClient installation, the endpoint user must connect FortiClient Telemetry to FortiGate or FortiClient EMS to receive the profile configuration and complete the endpoint management setup. See [Connecting manually from FortiClient on page 14](#).
7. View the endpoint status. See [Viewing endpoints on page 21](#).

FortiClient EMS integrated with FortiGate

Following is a summary of how to use FortiClient EMS when integrated with FortiGate:

1. Configure user accounts. See [Configuring user accounts on page 12](#).
2. Add domains and/or discover local endpoints. See [Adding endpoints on page 13](#).
3. Create gateway IP lists. See [Creating gateway IP lists on page 15](#).
4. Assign the lists to domains or workgroups. See [Assigning gateway IP lists to endpoints on page 16](#).
Alternately, you can add a FortiClient Telemetry gateway IP list to a custom FortiClient installer by using the FortiClient Configurator tool.
5. Add a FortiClient installer to EMS. See [Adding FortiClient installers on page 16](#).
6. Create an endpoint profile and select a FortiClient installer. See [Creating profiles to deploy FortiClient on page 18](#).



You can use FortiClient EMS with an Active Directory server to install and upgrade FortiClient on endpoints before and after endpoints connect Telemetry to EMS. You can use FortiClient EMS with workgroups only to upgrade FortiClient on endpoints after they connect Telemetry to EMS and FortiClient registers to FortiClient EMS. When using workgroups, you must separately install FortiClient on endpoints. See the *FortiClient EMS Administration Guide* for details.

7. Prepare Windows endpoints for FortiClient deployment. See [Preparing Windows endpoints for FortiClient deployment on page 21](#).
You must also prepare the Windows AD server for deployment. For details, see the *FortiClient EMS Administration Guide*.
8. Assign a profile to a workgroup or domain, an endpoint group, or an organizational group. See [Assigning profiles to endpoints on page 21](#).
Depending on the configuration of the selected profile, FortiClient will be installed on the endpoints to which the profile is applied.
After FortiClient installation, the endpoint user must connect FortiClient Telemetry to FortiGate or FortiClient EMS to receive the profile configuration and complete the endpoint management setup. See [Connecting manually from FortiClient on page 14](#).
9. View the endpoint status. See [Viewing endpoints on page 21](#).

Configuring user accounts

You can configure users to have no access to FortiClient EMS, or you can configure users to have administrator access to FortiClient EMS. You can configure local Windows users, LDAP users, or both local Windows users and LDAP users.

For local Windows users, the list of users is derived from the server on which FortiClient EMS is installed. If you want to add more users, you must add them to the server.

For LDAP users, you must add an LDAP server to FortiClient EMS, and then configure users.

To add an LDAP server:

1. Go *View > User Management*.
2. Click the *LDAP Server* tab.

3. Configure the options, and click *Test*.
4. If the test is successful, click *Save*.

To configure users:

1. Go to *View > User Management*.
2. On the *Administration* tab, click *+Add* from the toolbar.
3. In the *Add User* list, select *Windows User* or *LDAP User*.
The *LDAP User* options is available only after you add an LDAP server to FortiClient EMS.
4. Select the specific domain access for the user.
5. Configure the permissions.
6. Click *Save*.

Adding endpoints

You can add endpoints by using an Active Directory service. Endpoints are also added when endpoint users manually connect FortiClient Telemetry to FortiClient EMS.

Adding endpoints using an Active Directory domain server

Endpoints can be manually imported from an Active Directory (AD) domain server. You can import and synchronize information about computer accounts with an LDAP or LDAPS service. You can add endpoints by identifying the endpoint devices that are part of an AD domain server.



An instructional video on how to add a domain is available in the [Fortinet Video Library](#).



You have the option to add the entire domain or just an organizational unit (OU) from the domain.

To add endpoints using an Active Directory domain service:

1. Click *Endpoints > Add new domain*. The *Domain Settings* pane is displayed.

Domain Settings

Group Name required

Server IP/Name required

Server Port 389

Distinguished Name optional

Bind Type Simple Anonymous Regular

User DN

Password

☐ LDAPS Connection

2. Configure the following options:

Group Name	Enter a name for the group. The name will be displayed in the FortiClient EMS Endpoint view.
Server IP/Name	Type the IP address or name.
Server Port	Type the port number.
Distinguished Name	Type the distinguished name (optional).
Bind Type	Select the bind type: <i>Simple</i> , <i>Anonymous</i> , or <i>Regular</i> . When you select <i>Regular</i> , enter the <i>User DN</i> and <i>Password</i> .
User DN	Available when <i>Bind Type</i> is set to <i>Regular</i> . Type the user DN.
Password	Available when <i>Bind Type</i> is set to <i>Regular</i> . Type the user password.
Show Password	Available when <i>Bind Type</i> is set to <i>Regular</i> . Turn on and off to show or hide the password.
LDAPS	Turn on to enable a secure connection protocol when <i>Bind Type</i> is set to <i>Regular</i> .

3. Click *Test* to test the domain settings connection.
4. If the test is successful, select *Save* to save the new domain. If not, correct the information as required then test the settings again.

Connecting manually from FortiClient

Endpoint users can manually connect FortiClient Telemetry to FortiClient EMS by specifying the IP address for FortiClient EMS in FortiClient console. This process is sometimes called registering FortiClient to FortiClient EMS.

To connect FortiClient Telemetry to FortiClient EMS:

1. In FortiClient console on the endpoint device, go to the *Compliance* tab.
2. In the *FortiGate or EMS* box, type the IP address for EMS, and click *Connect*.
FortiClient registers to FortiClient EMS.

For more information about FortiClient, see the *FortiClient Administration Guide* available on the docs.fortinet.com site.



The FortiClient Telemetry gateway port may be appended to the gateway IP list address on FortiClient and separated by a colon. When the port is not provided, FortiClient attempts to register to the IP address given by using the default port. The default registration port in FortiClient 5.2 is 8010 and in FortiClient 5.4 is 8013. FortiClient EMS listens for registration on port 8013 by default.

Creating gateway IP lists

Gateway IP lists are useful when you are using FortiClient EMS integrated with FortiGate. If you are using FortiClient EMS without FortiGate, you are not required to use gateway IP lists.

You can create one or more gateway IP lists. Each list can contain IP addresses for multiple FortiGate units.

To create gateway IP lists:

1. Go to *Gateway IP Lists*.
2. Click the *Add a new IP list* button (the + icon).
3. Configure the following:

Name	Enter a name for the list.
Export XML	Available after you save the list. Click to export the list to a configuration file in XML format.
Comment	Enter additional comments (optional).
IP List	<p>Enter the IP address and port for FortiGate devices by using the following format: IP:port. You can also use a Fully Qualified Domain Name (FQDN).</p> <p>Click + to add additional IP addresses, and use the arrow keys to order the IP addresses in the list.</p>
Use Connection Key	Enable the registration key for FortiGate devices that FortiClient endpoints can use for registration.
Connection Key (Optional)	Enter the registration key.
Confirm Connection Key	Re-enter the registration key to confirm.
Monitored By EMS	Select an option from the dropdown list. Users can configure this IP address in the <i>View > Settings</i> page.

4. Click *Save*.
After you save the list, the *Export XML* button is displayed.

Assigning gateway IP lists to endpoints

After creating a gateway IP list, you can assign the list to endpoints. When you assign the IP list and FortiClient Telemetry data registration process has started, the endpoint will register to a FortiGate or EMS, based on the gateway IP list.

To assign gateway IP lists to endpoints:

1. Go to *Endpoints*.
2. Right-click a domain or workgroup, and select *Assign FortiClient Telemetry Gateway IP List*.
3. Select the desired list.

Adding FortiClient installers

When you add a FortiClient installer to FortiClient EMS, you can specify what FortiClient features to include in the installer for the endpoint. You can include a feature in the installer, then disable the feature in the profile. Because the feature is included in the installer, you can update the profile later to enable the feature on the endpoint.

When you add a FortiClient installer to FortiClient EMS, an installer for the Windows operating system and an installer for the OS X operating system are added to FortiClient EMS.



After you add a FortiClient installer to FortiClient EMS, you cannot edit it. You can delete the installer from FortiClient EMS, and edit the installer outside of FortiClient EMS. You can then add the edited installer to FortiClient EMS.

To add FortiClient installers:

1. Go to *View > Software Manager*. The *FortiClient Software Manager* pane is displayed.
2. Click the **+ Add** button.
3. On the *General* tab, set the following options:

Name	Type the FortiClient installer's name.
Notes	(Optional) Type any notes about the FortiClient installer.
FortiClient Version	Select the FortiClient version to install. Click <i>Upload</i> to add a custom FortiClient installer.
Patch Version	Select the specific FortiClient patch version to install.
Keep software updated to the latest patch release	Select to enable FortiClient to automatically update to the latest patch release when FortiClient is installed on an endpoint. This field is only available for the latest FortiClient version FortiClient EMS can access from FortiGuard. This option is not available if an older FortiClient version is selected.

4. On the *Components* tab, set the following options:

Security Fabric Agent (Mandatory Feature)	Enabled by default and cannot be disabled. Installs FortiClient with Telemetry and Vulnerability Scanning enabled.
Secure Access Architecture	Enable to install FortiClient with SSL VPN and IPsec VPN enabled. Disable to omit SSL VPN and IPsec VPN support from the FortiClient installer.
Additional Security Features	<p>Enable to select one, two, or all of the following features:</p> <ul style="list-style-type: none"> • AntiVirus • WebFiltering • Application Firewall • Single Sign-On mobility agent <p>Disable to exclude the features from the FortiClient installer.</p>

5. On the *Telemetry* tab, set the following options:

EMS	Click <i>EMS</i> to configure the FortiClient installer to connect Telemetry to EMS.
FortiGate	<p>Click <i>FortiGate</i>, and select the name of the gateway IP list to use. The gateway IP list defines the IP address for FortiGate and includes the IP address for EMS.</p> <p>You must define a FortiClient Telemetry gateway IP list to select FortiGate. If you have not created a list, the <i>No Gateway IPs have been defined</i> dialog box is displayed, and you can click <i>OK</i> to create a list.</p>

6. On the *Advanced* tab, set the following options:

Automatic registration	Enable to configure FortiClient to automatically connect Telemetry to EMS or FortiGate after FortiClient is installed on the endpoint. Disable to turn off this feature and require endpoint users to manually connect Telemetry to EMS or FortiGate.
Desktop shortcut	Enable to configure the FortiClient installer to create a desktop shortcut on the endpoint device.
Start menu shortcut	Enable to configure the FortiClient installer to create a Start menu shortcut on the endpoint device.

7. Click *Save*. The FortiClient installer is added to FortiClient EMS and displayed on the *FortiClient Software Manager* pane.

Configuring profiles

When you install FortiClient EMS, a default profile is created. This profile is applied to any groups that you create. The default profile is designed to provide effective levels of protection. If you want to use specific features, such as application firewall, you can create a new profile or change the default profile.

Consider the following when creating profiles:

- Use default settings within a profile.
- Consider the role of the endpoint when changing the default profile or creating new profiles.
- Create a separate group and profile for endpoints that require long-term special configuration.
- Use FortiClient EMS for all central profile settings, and set options for within the group instead of for the endpoint itself when possible.

Creating profiles to deploy FortiClient

You must create a new profile to deploy FortiClient to endpoints. You cannot add a FortiClient installer to the default profile.

You must add FortiClient installers to FortiClient EMS before you can select the installers in a profile. See [Adding FortiClient installers on page 16](#).

The selected FortiClient installer in a profile controls what tabs are displayed for configuration in the profile. Only the tabs for the features in the selected installer are displayed for configuration in the profile. For example, if the installer includes only the VPN feature, only the *VPN* tab is displayed for you to configure. The *System Settings* tab is always displayed.

You can disable a feature that is included in the installer, and then enable the feature in the profile at a later date. For example, if the installer includes the Web Filter and VPN features, you can disable the Web Filter feature and keep the VPN feature enabled. When FortiClient is installed on the endpoint, the Web Feature is installed, but disabled.

To create profiles for FortiClient deployment:

1. Go to *Endpoint Profiles*, and click the *Add a New Profile button* (the + icon). The *Creating New Profile* pane is displayed.
2. On the *Deployment* tab, enable *FortiClient Deployment*. The FortiClient Deployment options are displayed.
3. Set the following options on the *Deployment* tab:

Action		
	Assign an	Click <i>Installer</i> .
	Installer	<p>In the <i>Installer</i> list, select a FortiClient installer. If you have not added a FortiClient installer to FortiClient EMS, click <i>Create a New Installer</i>.</p> <p>The selected FortiClient installer affects what tabs are displayed for configuration. Only tabs related to features enabled in the FortiClient installer are displayed for configuration.</p>
Schedule		
	Start At	Specify what time to start the installation of FortiClient on endpoints.

	Prompt end user if a reboot is needed during installation	Enable to prompt the end user if a reboot of the endpoint device is needed. Disable to reboot the endpoint device without prompting the user. If no endpoint user is logged into FortiClient, the endpoint is rebooted without a prompt.
Credentials		
	Username	Type the username to perform deployment on AD. You must enter the admin credentials for the AD in the profile. Enter the appropriate credentials in the profile you will assign to the AD. The credentials allow EMS to install FortiClient on endpoints by using AD. If the credentials are wrong, the installation fails, and an error displays in EMS.
	Password	Type the password to perform deployment on AD.

- Set the options on the remaining tabs.
- Click *Save Profile* to save the profile.

Importing FortiGate profiles

In FortiOS, endpoint profiles are called FortiClient profiles. You can import a FortiClient profile into EMS, and then edit the profile in EMS to add a FortiClient installer or to add configuration information that supports the FortiGate compliance rules.



To import profiles successfully from FortiOS to FortiClient EMS, FortiGate must have the HTTPS port open. In FortiOS, go to *Network > Interfaces > Restrict Access > Enable checkbox for HTTPS*.

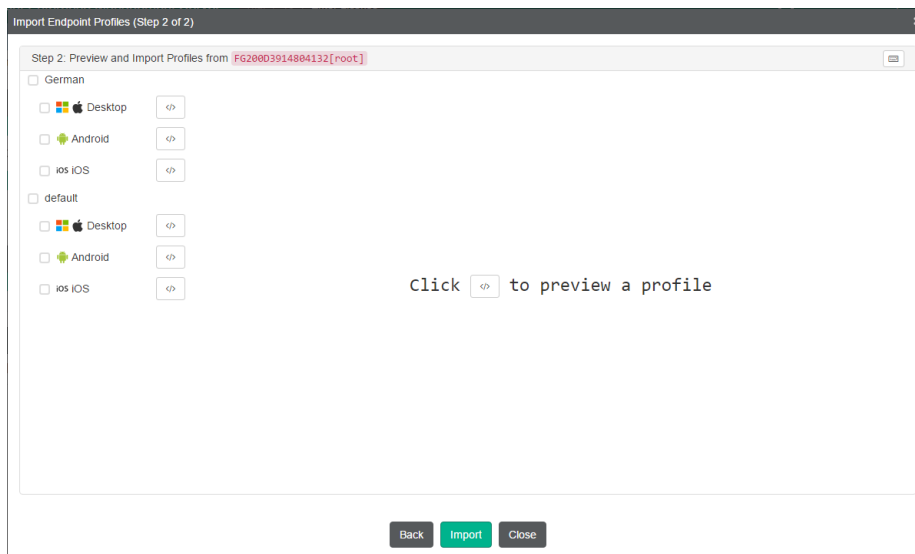
To import profiles:

- Click *Endpoint Profiles > Import Profiles from FortiGate*. The *Import Endpoint Profiles* window opens.

- Complete the following options, and click *Connect*.

IP Address/Hostname	Enter the IP address and port of the FortiGate device from which the profile is being imported, in the format: <ip address>:<port>.
VDOM	Enter a VDOM name from the FortiGate if applicable.
Username	Enter the login username for the FortiGate.
Password	Enter the login password for the FortiGate.

The list of FortiClient profiles configured on the FortiGate is displayed.



Under each profile name is the list of profiles created for different operating systems, such as desktops running a Windows or Mac operating system or devices running an Android operating system. For example, under the default profile, *Desktop*, *Android* and *iOS* profiles are listed. You can click the </> icon beside each profile to preview the settings in XML format.

3. Select the profiles to import into EMS and click *Import*.

Select the name of the profile to import all profiles for it into EMS. You can also clear the checkbox beside the profiles you do not want to import into EMS. For example, you can import the Desktop and iOS profiles, but not the Android profile for a given profile name.

The selected profiles are imported into EMS and display under the *Endpoint Profiles* pane in a group named after the FortiGate device from which they were imported.

4. In the *Endpoint Profiles* page, select an imported profile to edit it.

The options configured in the profile by the FortiGate administrator are read-only compliance rules. You cannot change them. You can edit additional options to provide configuration information to support the compliance rules. You can also add a FortiClient installer to the profile by using the *Deployment* tab. Custom installers can be created. See [Adding FortiClient installers on page 16](#).

5. Edit the options on the tabs.

6. Click *Save Profile*.

Preparing Windows endpoints for FortiClient deployment

The following services must be enabled and configured on each Windows endpoint before FortiClient is deployed to them:

- Task Scheduler: Automatic
- Windows Installer: Manual
- Remote Registry: Automatic



The Windows Firewall must be configured to allow the following inbound connections:

- File and Printer Sharing (SMB-In)
 - Remote Scheduled Tasks Management (RPC)
-

For AD group deployments, an AD administrator account is required. For non-AD deployments, the installer URL can be shared with users, who can then download and install FortiClient manually. You can locate the installer URL in Software Manager. Go to *View > Software Manager*.

Assigning profiles to endpoints

After creating the profile, you can assign the profile to domains or workgroups. When you assign the profile to domains or workgroups, the profile settings are automatically pushed to the endpoints in the domain or workgroup.

If you do not assign a profile to a specific domain or workgroup, the default profile is automatically applied.

To assign profiles:

1. Go to *Endpoints*
2. Right-click a domain or group, select *Assign profile*, and then the profile. A confirmation dialog box is displayed.
3. Click *Yes*. The profile is assigned.

Viewing endpoints

After you add endpoints to FortiClient EMS, you can view the list of endpoints in a domain or workgroup in the *Endpoints* pane. You can also view details about each endpoint in the *Client Details* pane and use filters to access endpoints with specific qualities.

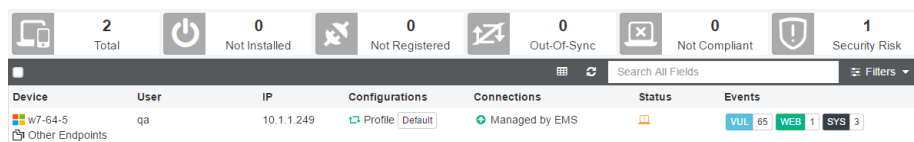
Viewing the Endpoints content pane

You can view information about endpoints on the *Endpoints* content pane.

To view the Endpoints content pane:

1. Go to *Endpoints*, and select a domain or workgroup.

The list of endpoints in FortiClient EMS is displayed in the content pane as well as a quick status bar and a toolbar.



Total	Number of endpoints. Click to display the list.
Not Installed	Number of endpoints that do not have FortiClient installed. Click to display the list of endpoints without FortiClient installed.
Not Registered	Number of endpoints that are not registered to either FortiClient EMS or FortiGate. Click to display the list of unregistered endpoints.
Out of Sync	Number of endpoints that have an out of sync profile. Click to display the list of endpoints with out of sync profiles.
Not Compliant	Number of endpoints not compliant with the FortiGate compliance rules. Click to display the list of not compliant endpoints.
Security Risk	Number of endpoints that are a security risk. Click to display the list of endpoints.
Checkbox	Click to select all endpoints that are displayed in the content pane.
Show/Hide Heading	Click to hide and display the following column headings: <i>Device</i> , <i>User</i> , <i>IP</i> , <i>Configurations</i> , <i>Connections</i> , <i>Status</i> , and <i>Events</i> .
Refresh	Click to refresh the list of endpoints in the content pane.
Search box	Type a value and press <i>Enter</i> to search for the value in the list of endpoints.
Filters	Click to display and hide the filters that you can use to filter the list of endpoints for the selected domain or workgroup.
Device	Visible when headings are displayed. Displays an icon to represent the operating system on the endpoint as well as the name of the device.
User	Visible when headings are displayed. Displays the name of the user logged into the endpoint.
IP	Visible when headings are displayed. Displays the IP address for the endpoint.
Configurations	Visible when headings are displayed. Displays the name of the profile assigned to the endpoint and the synchronization status of the profile.

Connections	Visible when headings are displayed. Displays whether the endpoint is connected to FortiClient EMS or FortiGate and the connection status of <i>Online</i> , <i>Offline</i> , or <i>Not Registered</i> .
Status	Visible when headings are displayed. Displays one of the following compliance statuses for the endpoint. <ul style="list-style-type: none"> • Compliant • Not compliant • Not participating in compliance • Quarantined • Excluded • Not registered • Not installed
Events	Visible when headings are displayed. Displays FortiClient events for the endpoint.

2. Click an endpoint to display more details about it in the content pane.

The following dropdown lists are displayed in the toolbar for the selected endpoint:



Checkbox	Click to select and deselect all endpoints in the content pane. You can then select or clear the checkbox for individual endpoints to fine tune the list of selected endpoints.
Scan	Click to start a Vulnerability or AntiVirus scan on the selected endpoint.
Patch	Click to patch all critical and high vulnerabilities on the selected endpoint. Choose one of the following options <ul style="list-style-type: none"> • Selected Vulnerabilities on Selected Clients • Selected Vulnerabilities on All Affected Clients • All Critical and High Vulnerabilities
Action	Click to perform one of the following actions on the selected endpoint: <ul style="list-style-type: none"> • Upload FortiClient Logs • Request Diagnostic Results • Update Signatures • Re-register • De-register • Register • Quarantine • Un-quarantine • Exclude from Management • Mark as Uninstalled • Delete Device

The following tabs are available in the content pane toolbar when you select an endpoint:

Summary Antivirus Events Firewall Events Vulnerability Events Web Filter Events System Events

Summary	
<user name>	Displays the name of the user logged into the selected endpoint.
Device	Displays the device name for the selected endpoint.
OS	Displays the operating system and version for the selected endpoint.
IP	Displays the IP address for the selected endpoint.
MAC	Displays the MAC address for the selected endpoint.
Last Seen	Displays the last date and time that FortiClient sent a keep-alive message to EMS. This information is useful if FortiClient is offline because it indicates when the last keep-alive message occurred.
Location	Displays whether the selected endpoint is onnet or offnet.
Connection	Displays when the selected endpoint is connected to FortiClient EMS or FortiGate. Also displays the status of the connection.
Configuration	Displays the following information for the selected endpoint: <ul style="list-style-type: none"> • Profile: Name of the profile assigned to the selected endpoint • Installer: Name of the FortiClient installer used for the selected endpoint. Displays <i>Not Assigned</i> if no FortiClient installer has been assigned to the selected endpoint. • IP List: Name of the gateway IP list used for the selected endpoint. Displays <i>Not Assigned</i> if no gateway IP list has been assigned to the selected endpoint. • FortiClient Version: Version of FortiClient installed on the selected endpoint.
Compliance	Displays if the endpoint is compliant. If the endpoint is not compliant, displays the features for which FortiClient is not compliant.
Features	Displays which features are enabled for FortiClient.
Antivirus Events	
Date/Time	Displays the date and time of the antivirus event.
Message	Displays the message for the antivirus event.
Firewall Events	
Date/Time	Displays the date and time of the firewall event.
Message	Displays the message for the firewall event.
Vulnerability Events	

Vulnerability	Displays the name of the vulnerability. For example, <i>Security update available for Adobe Reader</i> .
Category	Displays the vulnerability's category. For example, <i>Third Party App</i> .
Application	Displays the name of the application with the vulnerability.
Severity	Displays the severity of the vulnerability.
FortiGuard ID	Displays the FortiGuard ID number. If you click the FortiGuard ID number, it will redirect you to FortiGuard where further information will be provided if available.
Bulletin	Displays a link to a bulletin about the software vulnerability.
Web Filter Events	
Date/Time	Displays the date and time of the web filter event.
Message	Displays the message for the web filter event.
System Events	
Date/Time	Displays the date and time of the system event.
Message	Displays the message for the system event.

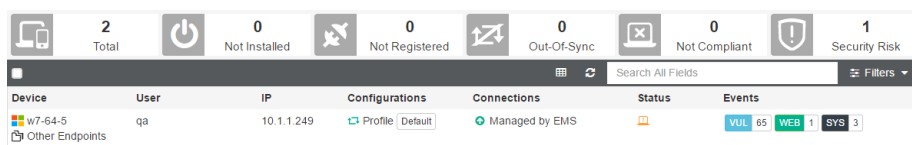
Using the quick status bar

You can use the quick status bar to quickly display filtered lists of endpoints on the *Endpoints* content pane.

To use the quick status bar:

1. Go to *Endpoints*.
2. Click a domain or workgroup.

The list of endpoints is displayed as well as the quick status bar.



3. Click one of the following buttons in the quick status bar:
 - Total
 - Not Installed
 - Not Registered
 - Out-Of-Sync
 - Not Compliant
 - Security Risk

The list of affected endpoints is displayed.

- Click an endpoint to display details about the endpoint.
- In the *Events* column, click the *Vul<number>*, *Web <number>*, *SYS<number>*, *AV<number>*, and *FW<number>* buttons to display the associated tab of details for the selected endpoint.
- Click the *Total* button to clear the filters.
The unfiltered list of endpoints is displayed.

Viewing endpoint details

You can view details for each endpoint on the *Endpoints* content pane. For a description of the options on the Endpoints content pane, see [Viewing the Endpoints content pane on page 21](#).

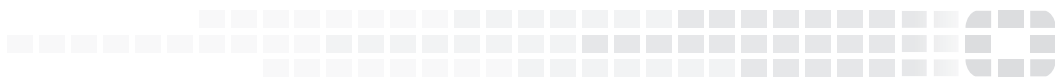
To view endpoint details:

- Go to *Endpoints*, and select a domain or workgroup.
The list of endpoints for the selected domain or workgroup is displayed.
- Click an endpoint to display more details about it in the content pane.
Details about the endpoint are displayed in the content pane.

The screenshot displays the Fortinet FortiGate GUI's endpoint management interface. At the top, a summary bar shows counts for various states: 2 Total, 0 Not Installed, 0 Not Registered, 0 Out-Of-Sync, 0 Not Compliant, and 1 Security Risk. Below this is a table with columns for Device, User, IP, Configurations, Connections, Status, and Events. The selected endpoint 'qa' (techdoc-fclient) is highlighted. The main content area provides detailed information for 'qa', including its device type, OS (Microsoft Windows 8.1), IP (172.17.60.166), MAC (00-15-5d-6c-69-1b), last seen time (5/18/2017, 1:10:49 PM), and location (On Net). It also shows connection status (Managed by EMS), configuration details (Profile: Default, Installer: Not Assigned, IP List: Not Assigned, FortiClient Version: 5.6.0.1057), and compliance features (AntiVirus installed, Sandbox Detection installed, Web Filter enabled, Application Firewall installed, Remote Access installed, Vulnerability Scan enabled, SSOMA installed). At the bottom, a secondary bar shows counts for VUL (65), WEB (1), and SYS (3).



FORTINET®



Copyright© 2017 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.